CA Unified Infrastructure Management Server

Release Notes and Upgrade Guide

8.0

ca technologies

Contents

Chapter 6: NMSRN--Fixed Defects   39

Chapter 1: New and Changed Functionality

Unified Infrastructure Management (UIM) Server (formerly *Nimsoft Monitor Server*) 8.0 is a major release that improves on the stability, scalability, performance, features and functionality of the product, adding these significant new features.

Installation

- New names for the UIM Server installers:

  setupCAUIMServer.exe
  setupCAUIMServer_linux.bin
  setupCAUIMServer_solaris_sparc64.bin
  setupCAUIMServer_solaris_x64.bin

- The installer screens and UIM Server 8080 webpage have been updated.

Hub and Root

- New robot configuration options to support marketplace probes.

- New queue status alarms provide improved alarms for tunnels. Because hub 7.xx tunnel connections now automatically reset when network conditions are poor, alarms based simply on a low-level tunnel's state at a given instant no longer provide value. Those alarms have been replaced with more powerful queue status alarms, which can more accurately track and provide alerts on the on-going quality of the higher-level connection.

- Improved robot behavior regarding the *origin* attribute:

  - When a robot fails over from its primary hub to a secondary hub, it now retains the origin of the primary hub.

  - If a robot's origin changes for any reason, all of the robot's probes are restarted to pick up the change in origin.

- Hub 7.61 provides improved performance and is a usable and viable upgrade from hub 5.82:

  - Inbound and outbound message processing is independently multi-threaded.

  - Hub can handle higher throughput per queue and/or a higher number of queues at a fixed throughput.

  - Hub startup and overall through put is faster and hubs are more stable due to smarter disk file handling and file chunking.

Automated Deployment Engine

- ADE 2.0 is a Java-based redesign of distsrv with scalability, flexibility, and maintainability in mind.

- Admin Console now uses ADE for package deployment, which is two to five times faster than with distsrv. (Infrastructure Manager continues to use distsrv).

- ADE uses an archive cache to do quick package lookups and file extractions. Files that have been extracted are maintained in a cache to speed up package deployment. This cache is cleared at startup.

- ADE Archive stays in sync with file system, and the archive-sync solution is much more scalable than distsrv package forwarding. Processing is distributed, rather than going through a single master distsrv.

Data_engine

- Data table partitioning and index maintenance for Oracle databases are supported.

- The statistics display table in the Admin Console data_engine configuration GUI now includes daily and baseline statistics.

Discovery

- USM displays more detailed agent status during the discovery phase.

- Discovery Wizard and Discovery Agent support seed device discovery. When entering ranges in the wizard, if you specify information about one or more "seed" devices, discovery agent can:

  – Automatically discover the local subnets that it collects from the seed devices.

  – Find devices connected to the seed devices, which accelerates the discovery of known devices on the network.

- Enabled integration with CA Capacity Management by providing more detailed processor attributes for host systems discovered with WMI, SSH, or SNMP credentials. Note that WMI and SSH provide more detailed processor information than SNMP. The new host system attributes published by the discovery agent are:

  – ProcessorDescription

  – NumberOfPhysicalProcessors

  – NumberOfProcessorCores

  – NumberOfLogicalProcessors

Chapter 2: Requirements

Supported Systems

For information on:

- System requirements, see the Installation Guide.

- Supported operating systems, databases, JRE versions, and browsers, see the Compatibility Support Matrix.

- Components that are being deprecated or are no longer supported, see the End of Sales and Support Announcements.

- **Note:** NMS 6.5 and later requires a 64-bit version of a supported operating system. If you are migrating from a 32-bit system, contact Support for assistance.

Core Components

The UIM infrastructure (hubs, robots, and probes) is supported on Windows, AIX, HP-UX, Linux, and Solaris. To see which versions are supported, see the Compatibility Support Matrix.

Additional System Requirements

Data Engine

Data Engine requires:

- libstdc++.so.5 (libstdc++-3.3.4-11.x86_64.rpm) on OpenSUSE Linux distributions
- Windows 2008 R2 SP1 on Windows distributions

The Admin Console data_engine configuration GUI allows you to partition your Oracle database. The partitioning process:

- Requires enough free disk space to create a partitioned interim table.
- Copies the contents from the original data tables into the interim data tables, swaps the original data tables and interim data tables, and finally deletes the original data tables.

Before you partition your Oracle database, determine the size of the largest unpartitioned RN table to determine how much free disk space is needed to complete this task. For details, refer to "Preparing to Partition Your Oracle Database" in the Admin Console *Probe Guide for Data Engine*.

Database

- The database must be case insensitive when handling queries.
- Database free space check is not implemented for Oracle and MySQL.

Discovery

If you want Discovery to locate IPv4 and IPv6 systems, discovery_agent must run on dual-stack IPv4/IPv6 system.

Supported Languages

UIM Server is available in English, German, Spanish, Brazilian Portuguese, Simplified Chinese, Japanese, and Korean.

Chapter 3: Considerations

This section describes characteristics found in this release that affect the installation, upgrade, localization, or general behavior of UIM Server 8.0.

Topics:

Required Login Privileges

Use a login with *administrator* or *root* privileges when installing or upgrading UIM Server.

Install Two or More Hubs

We recommend that you install at least two hubs on the same domain and network so that if the server hosting your primary hub fails, you do not lose user and security data (user definitions, ACLs, etc.). With more than one hub, this information is mirrored between the hubs.

Clock Synchronization and Maintenance Schedules

To ensure that maintenance schedules start and stop at the intended times, the system clocks on the following servers must be synchronized:

- UIM Server system (primary hub, this includes the maintenance_mode probe)

- Database server

- NAS server(s)

- UMP server(s)

Out-of-synch clocks can result in erroneous or missing alarms. For example, suppose the clock on the UMP server is 30 minutes ahead of the NAS server. You place your web server in a maintenance schedule that goes from 9:00 to 11:00.

- At 9:00, you take the web server offline for maintenance. Because the NAS server's time is 8:30, it does not suppress alarms at the anticipated time.

- At 11:00, you bring the web server back online. However, because the NAS server's time is 10:30, it will suppress alarms for another 30 minutes.

For information on using the Network Time Protocol (NTP) to synchronize your servers, go to the NTP distribution site at http://doc.ntp.org.

Upgrade the Probe Provisioning Manager (ppm)

To ensure that you have access to the latest Admin Console functionality, we recommend you download the latest version of the ppm probe (probe provisioning manager) to all hubs within your domain *after* you update UIM Server. Use either Admin Console or Infrastructure Manager to deploy the ppm probe from the probe archive on the Support web site.

QoS Processor Insert Rate and Java Heap Size

Under normal operation, the maximum insert rate on a system where qos_processor and data_engine run together is 15,000 inserts per second. The actual maximum insert rate will vary based on the performance of the hardware. This rate is largely independent of the database type.

The memory footprint of the qos_processor probe directly correlates with the size of the S_QOS_DATA table in the database. Set the maximum Java heap size appropriately:

Number of QoS objects	Maximum Java heap size
Less than 300,000	1 GB (default)
300,000 – 1,000,000	1.5 GB
More than 1,000,000	2.5 GB

Chapter 4: Upgrading to UIM Server 8.0

This section explains how to upgrade to UIM Server 8.0.

This process consists of a chain of updates to the modules you currently have installed. Note the following:

- Do **NOT** restart your system until all modules have been installed, even if the system prompts you to restart at intermediate points in the process.

- Upgrade UIM Server before you upgrade UMP. This ensures that UMP's required database schema is in place.

- For supported upgrade paths, refer to the compatibility support matrix.

Upgrading UIM Server

Because your existing configuration is retained when you upgrade, an upgrade is much simpler than a new installation.

Before you begin, ensure that you follow a supported upgrade path described in the Compatibility Support Matrix.

To upgrade UIM Server, you must:

1. Perform any tasks in Before You Upgrade (see page 15) that are appropriate for your deployment.

2. Run the UIM Server installer with the **Upgrade** option. Select the appropriate installation mode for instructions:

   ■ GUI mode (see page 18) provides a graphical user interface on Windows, Linux and Solaris.

   ■ Console mode (see page 17) provides a command-line interface on Linux and Solaris.

   ■ Silent mode (see page 18), available on Windows, Linux and Solaris, allows you to specify installation parameter values in a file that is used to complete the install with no user interaction.

When you upgrade, your existing configuration is retained, making an upgrade much simpler than a new installation.

Upgrading on a Microsoft Cluster Server

To upgrade UIM Server on a Microsoft Server 2003/2008/2008 R2 failover cluster:

1. Upgrade the primary (active) node using either the GUI mode (see page 16) or silent mode (see page 18) procedure.

2. Make the secondary (passive) node active, then upgrade the node using the same process you used on the primary node.

This ensures that registry keys on both the primary (active) and secondary (passive) nodes are updated for the new version.

Before You Upgrade

The UIM Server installer lets you easily upgrade in GUI, console, or silent mode. When you upgrade, your configuration (domain and hub names, IP addresses, user accounts, passwords, etc.), is retained. Perform the following tasks before you run the installer.

All Deployments

- **Verify the upgrade path** (required)

  Ensure that you follow a supported upgrade path described in the Compatibility Support Matrix.

- **Disable package forwarding and clear the distsrv job queue** (required)

  Package forwarding is configured in the distsrv probe GUI. To view the queue, select **Tools > Distribution** in Infrastructure Manager. The upgrade will fail if the distsrv job queue has jobs pending. After a successful upgrade, re-enable package forwarding in distsrv if desired.

- **Remove customized probes in your probe archive** (recommended)

  Move or delete customized probes in your probe archive; leave the basic infrastructure probes. After all installations and upgrades are complete (especially those for UMP and Unified Reporter), you can selectively move the probes back into the archive.

- **Back up the primary hub configuration** (recommended)

  Save a copy of the hub.cfg file in the *<UIM_Server_install>*\hub folder. Optimal timeout parameters for the updated hub are set during the update, overwriting existing timeout settings. CA recommends running the updated hub with these optimal values for improved performance. However, if you wish to revert to the old timeout settings for any reason, keep a backup of the old Hub configuration file.

Windows

- Install Service Pack 1 on Windows 2008 systems.

MS SQL Server

- Turn off index maintenance in data engine. On very large tables (over 10 GB), running index maintenance will take longer than expected. We recommend that users disable this feature when upgrading to 8.0, then re-enable it to run during off-peak hours, carefully monitoring the index maintenance processes. This configuration can be done in Admin Console or Infrastructure Manager.

Oracle

- As SYSDBA, execute:

  ```
  grant execute on dbms_redefinition to <NMS USER>;
  ```

- Turn off and purge the Oracle recycle bin.

  Important! If you are upgrading from NMS 7.5, the upgrade will fail if you do not purge the recycle bin.

  1. Use a tool such as SQL Developer to connect to the Oracle database.

  2. Purge the recycle bin. Execute:
     ```
     PURGE DBA_RECYCLEBIN
     ```

  3. Disable the recycle bin. Execute:
     ```
     ALTER SYSTEM SET recyclebin = OFF DEFERRED;
     ALTER SESSION SET recyclebin = off;
     ```

  4. Verify that the recycle bin is off. Execute:
     ```
     show parameter recyclebin;
     ```

GUI Mode Upgrade

Follow these steps:

1. Turn off any anti-virus scanners running on the server (these scanners can significantly slow down the installation).

   Note: Turn the anti-virus scanners on again immediately after installation.

2. Ensure you have disabled package forwarding and cleared the distsrv job queue (required) and removed customized probes in your probe archive (recommended).

3. Log in to Customer Support and go to **Downloads**.

4. Download and run the most recent UIM Server install package for Windows.

   Important: All fields in the installer dialogs are case-sensitive.

5. Follow the prompts to complete the installation. Where possible, the Installer displays the current configuration values for your confirmation.

6. When the upgrade is complete, make sure you:

   - Turn on anti-virus software

   - Enable package forwarding

   - Move customized probes back into your probe archive if necessary

Console Mode Upgrade (Linux and Solaris)

Follow these steps:

1. Turn off any anti-virus scanners running on the server (these scanners can significantly slow down the installation).

   Note: Turn the anti-virus scanners on again immediately after installation.

2. Ensure you have disabled package forwarding and cleared the distsrv job queue (required) and removed customized probes in your probe archive (recommended).

3. Log in to Customer Support and go to **Downloads**.

4. Download and run the most recent UIM Server install package for Linux or Solaris (the package is over 1 GB, so this could take several minutes).

5. Execute **chmod 755** on the install file to make it executable.

6. Run the installer. From a command line, execute:

   ■ Linux: **setupCAUIMServer_linux.bin -i console**

   ■ Solaris: **setupCAUIMServer_solaris_sparc64.bin -i console** or **setupCAUIMServer_solaris_x64.bin -i console**

7. Follow the prompts to complete the installation. Where possible, the Installer displays the current configuration values for your confirmation.

8. When the upgrade is complete, make sure you:

   ■ Turn the anti-virus scanners on again if necessary

   ■ Enable package forwarding

   ■ Move customized probes back into your probe archive if necessary

Silent Mode Upgrade

Follow these steps:

1. Turn off any anti-virus scanners running on the server (these scanners can significantly slow down the installation).

   Note: Turn the anti-virus scanners on again immediately after installation.

2. Ensure you have disabled package forwarding and cleared the distsrv job queue (required) and removed customized probes in your probe archive (recommended).

3. Log in to Customer Support and go to **Downloads**.

4. Download and run the most recent UIM Server install package for Windows.

5. Go to the **Downloads** tab at Nimsoft Technical Support. Under *CA Unified Infrastructure Management*, click the link for the current version of CA UIM Server, and download the:

   ■ Most recent **UIM Server installer package** for your operating system (the package is over 1 GB, so this could take several minutes)

   ■ **Silent Install Templates for UIM Serve**r zip package

6. On Linux or Solaris, execute **chmod 755** on the install file to make it executable.

7. Prepare your response file:

   a. Extract the silent install templates.

   b. Locate the **installer.upgrade.properties** file and save it as **installer.properties** in the same directory as the installer.

   c. Add your UIM administrator password to the **NMS_PASSWORD=** line in **installer.properties**.

   d. Save the file, ensuring the file type is still *PROPERTIES*. If the file type is *Text Document*, remove the **.txt** extension (which may not be displayed in the folder).

8. Run the installer. From a command line, execute:

   ■ Windows: **setupCAUIMServer.exe -i silent**

   ■ Linux: **setupCAUIMServer_linux.bin -i silent**

   ■ Solaris: **setupCAUIMServer_solaris_sparc64.bin -i silent** or **setupCAUIMServer_solaris_x64.bin -i silent**

9. The installer unpacks the files and completes the installation. This process can take several minutes or more. To see the progress of the installation, execute:

   ```
   tail -f /tmp/ia/iaoutput.txt
   ```

10. UIM Server launches. If for some reason it does not, execute:

   ■ Windows: **net start Nimsoft Robot Watcher**

   ■ Linux or Solaris: **/etc/init.d/nimbus start**

The upgrade is complete. After you upgrade, make sure you:

   ■ Turn anti-virus software

   ■ Enable package forwarding

   ■ Move customized probes back into your probe archive if necessary

Upgrading Secondary Hubs and Robots

Updating Infrastructure Manager

Upgrade Infrastructure Manager to the newest version. To see if it is installed, select **Start > All Programs > Nimsoft Monitoring**.

1. On the system where Infrastructure Manager in installed, browse to the UIM Server web page: *<UIM_Server_name_or_IP>*:8080.

2. Click **Legacy Infrastructure Manager** to install the new version on that machine.

Note: Admin Console provides a platform-independent alternative to Infrastructure Manager. It can be launched stand-alone in a browser at *<UIM_Server_name_or_IP>*:8080\adminconsole, or it can be run as a portlet within UMP.

Upgrading Hubs

1. Identify the systems that contain a secondary hub (view them in Admin Console or Infrastructure Manager; confirm by checking **Control Panel > Add/Remove Programs** on the system itself).

    Note: Updating secondary hubs is necessary only if you are updating from two or more versions back. Compare the component versions in [Verification of Successful Installation or Upgrade](#) (see page 22) to the versions currently installed secondary hubs.

2. On each system you identify:

    a. Save a copy of *hub.cfg* in the Nimsoft\hub folder. Optimal timeout parameters for the updated hub are set during the update, overwriting existing timeout settings. We recommend that you run the updated hub with these optimal values for improved performance. If you want to revert to the old timeout settings, rename the old configuration file back to hub.cfg.

    b. Browse to your NMS web page (http://*<servername_or_IP_address>*:8080).

    c. Download the installer:

    - ■ Windows: **Windows Robot, Hub, Distribution Server**

    - ■ Linux: **UNIX/LINUX installation utility (nimldr) for all platforms**

    d. Launch the installer and follow the prompts to complete the installation.

Updating Hub Queues for Discovery

If all discovery components are deployed only on the primary hub, communication is handled automatically and no queue configuration is required. However, if you distribute any discovery components to secondary hubs, you need to configure queues to ensure that information from the distributed probes can reach the discovery_server.

You can do this with a combination of *attach* and *get* queues, or with *post* queues. For instructions, refer to the *Discovery User Guide* in the UIM [documentation library](#).

Upgrading Robots

You can update all robots in your domain (including the robots on secondary hubs) with Admin Console or Infrastructure Manager, or by manually running an installer.

Admin Console:

1. Log in to Admin Console:
   http://*<UIM_Server_name_or_IP>*:8080/adminconsole

2. Locate the **robot_update** package in the **Archive**.

3. Drag and drop the package onto the icon of the robot you want to update.

Infrastructure Manager:

1. Launch Infrastructure Manger on your upgraded primary hub (or another hub with an updated archive).

2. Locate the **robot_update** package in the **Archive**.

3. Drag and drop the package onto the icon of the robot you want to update.

Manual installation:

On the system containing the robot you want to update, browse to your UIM Server web page:
http://*<UIM_Server_name_or_IP>*:8080

1. Download the appropriate installer:

   - Windows: **Windows Robot**

   - UNIX/Linux: **UNIX/LINUX installation utility (nimldr) for all platforms**

2. Launch the installer and follow the prompts to complete the upgrade.

Verification of Successful Installation or Upgrade

CA recommends you check the results of the installation process in order to detect any failure(s). Two indications of success:

- You see **Unified Infrastructure Management 8.0** on the UIM Server web page.

- You have current versions of all primary hub components:

    - Verify probe versions in Admin Console.

    - Select **Help > About** to check interface versions.

Note: These tables list the version numbers of probes provided with UIM Server 8.0. On occasion, CA provides newer versions of certain probes between server package releases. The latest probe updates are placed on the **Download** and **Archive** pages on the Support website as they are made available.

Important: During an upgrade, the installer overwrites currently installed probes and components. If "hot fix" probes or special/updated versions of components were installed to solve issues or to support customized requirements, upgrading can result in component downgrades. If this happens, the required components and probe versions can be restored by locating them in the UIM Server Archive, and installing them in place of what the upgrade provided.

User interfaces	Version 8.0	Prior release
Infrastructure Manager	4.08	4.08
Admin Console	8.00	7.60
Dr. Nimbus	1.5.3	1.5.3
Core components	**Version 8.0**	**Prior release**
alarm_enrichment	4.40	4.36
audit	1.22	1.22
automated_deployment_engine	2.00	1.31
baseline_engine	2.34	2.20
controller	7.62	7.60
data_engine	8.0	7.95
distsrv	5.30	5.30
fault_correlation_engine	1.66	1.66
hdb	7.62	7.60
hub	7.61	7.50

nas	4.40	4.36
nimldr	3.57	3.57
nis_server	3.26	3.22
maintenance_mode	8.00	1.10
mpse	1.63	1.60
ppm	2.38	2.31
prediction_engine	1.01	NA
qos_processor	1.23	1.23
relationship_services	1.70	1.70
robot_update	7.62	7.60
service_host	8.00	7.60
sla_engine	3.63	3.62
spooler	7.62	7.60
Discovery components	**Version 8.0**	**Prior release**
ace (multiplatform version)	3.40	3.20
assetmgmt	1.24	1.24
cisco monitor	3.36	3.36
cm_data_import	7.60	7.60
cdm	4.91	4.81
discovery_agent	8.00	7.60
discovery_server	8.00	7.60
interface_traffic	5.33	5.33
net_connect	3.04	3.02
rsp	4.01	4.00
topology_agent	1.69	1.69

Chapter 5: Known Issues

This section describes known issues and workarounds in some cases.

Performance, Stability, Scalability

Admin Console Returns a Null Pointer Exception After Package Download

After using Admin Console to download a package from the web archive, you might see the following error:

```
ServerErrorException - Internal Server Error:
'java.lang.NullPointerException'
```

Occasionally, this error might display when the file transfer rate is slow, the network is experiencing performance issues, or due to large files.

If the package appears in your local archive, then the download was successful and the error can be ignored. If the download failed, try to download the package again in Admin Console, or download it with Infrastructure Manager.

Controller Process Size Increase

On some platforms, the process size of the robot (specifically, the controller process) has increased, due to linking of additional libraries to support internationalization. The linking is to shared libraries, so actual memory usage on the system is not likely to increase. The actual memory used by the controller may also see a step increase as result of this new functionality, but the process size should be stable.

WMI and SSH Discovery Provide More Detailed Host System Information than SNMP

For network devices such as routers and switches, SNMP is the sole source for detailed discovery information. For host systems such as Windows, Unix, or Linux servers, it is recommended that you use WMI or SSH discovery instead of, or in addition to SNMP. While SNMP provides detailed network information for devices and systems, the host system information available from SNMP, such as processor attributes, is less complete than the information obtained from WMI or SSH discovery. Specifically:

- **ProcessorDescription** may not provide a meaningful value. Windows and Linux systems should provide meaningful values for this attribute, but Solaris systems may provide a generic value.

- **ProcessorSpeedInGhz, NumberOfPhysicalProcessors, NumberOfProcessorCores,** and **NumberOfLogicalProcessors** are not available from SNMP.

- **MemoryInGB** is set only for devices that implement the HOST-RESOURCES-MIB.

- **Model** is not set for host systems. This attribute is provided by the ENTITY-MIB, which is typically not implemented by host systems.

- The hardware vendors for Windows and Linux systems are Microsoft and NetSNMP, respectively.

Baseline Engine Sub System ID

The subsystem IDs in the dynamic threshold alarms generated from the baseline engine might not match the subsystem IDs in the static alarms generated from the probes.

Robot Functionality

Robot 7.10 (the controller, spooler and hdb probes) exhibited issues in a few distinct environments. If you are successfully using version 7.10, you can continue to use it after upgrading to UIM Server 8.0. If you are experiencing problems with version 7.10, we recommend you upgrade your robots to version 7.62.

Hub Performance in High Volume Deployments

In high-volume deployments, hub 7.10 may have issues when used as an LDAP proxy hub or when used with the SNMPCollector probe. These problems have been addressed in hub version 7.11 and later.

Potential Impact of Inactive Queues with Tunnels

When hub 7.10 is used a tunnel server, the number of resources used for Windows file handles and Unix file descriptors may grow steadily over time. The growth rate increases greatly when the tunnel server is servicing one or more *get* queues that carry little or no data, and therefore reset regularly. As the number of resources in use becomes large, the hub may automatically restart and return to normal operation. No data loss is expected during these restarts, and the system should automatically return to normal operation.

These problems have been addressed in hub version 7.11 and later.

Automated Deployment Engine (ADE)

ADE robot distribution to Windows targets sometimes fails to activate the hdb and spooler probes.

To resolve this issue, go to the affected system and do a **validate security** on the affected probes (hdb and spooler).

Slow Restart of discovery_server on MySQL

When Discovery Server starts, it executes a script to check/create tables in the database. A bug in MySQL 5.5 causes this script to run slowly (see Changes in MySQL 5.6.13 (2013-07-31 and MySQL Bug: Create Table If Not Exists).

Upgrading MySQL to version 5.6.13 or later resolves the issue.

When using the 5.5 stream of MySQL, the workaround is to turn off dashboard_engine and terminate any outstanding queries when restarting discovery server--this allows the discovery creation script to proceed.

Red Hat Enterprise Linux (RHEL)

UIM processes on RHEL 6.1 x86-64 consume more memory than on other Linux platforms.

- **RHEL v6 64-bit systems**

   Processes can take up to three times the amount of virtual and resident memory per process compared to previous releases of RHEL or other operating systems.

- **RHEL v6 32-bit systems**

   Processes can take several times more virtual memory, but resident memory per process is roughly equivalent.

Usability

Unable to Log In to Admin Console after Upgrading UIM Server

Problem:

When you enter the administrator user name and password on the Admin Console sign-in page, you see this error:

Unable to Sign In. Check the user name and password you entered are correct and try signing in again.

This issue occurs only in deployments that use MS SQL Server with Windows authentication.

Cause:

The service_host probe cannot find the path to the SQL Server JDBC Driver (sqljdbc_auth.dll). The log file (C:\Program Files (x86)\Nimsoft\probes\service\service_host\ service_host.log), will have entries that contain the following:

WARNING: Failed to load the sqljdbc_auth.dll

SEVERE: Login Error 2: Cannot create PoolableConnectionFactory. (This driver is not configured for integrated authentication.)

Workaround:

Add the path to the SQL Server JDBC driver to the service_host configuration.

1. Open Infrastructure Manager and log in to the domain as an administrator.

2. Right-click on the service_host probe and select **Configure**.

3. In the Raw Configure utility, click the **setup** folder, select the **CATALINA_OPTS** key, then click **Edit Key**.

4. Append the following to the key value:
   `-Djava.library.path="../../../lib"`

   Note: Make sure to leave a blank space between command line options.

5. Click **OK** to save the new key value, then click **OK** to save the configuration. The service_host probe automatically deactivates, then activates and applies the new configuration.

Unable to Log In to Admin Console

Problem:

You are unable to access a new or open session of Admin Console, or you see an error similar to:

> "ServerErrorException — Internal Server Error: '(12): login failed, Received status (12) on response (in sendRcvLogin) for cmd = 'login''

In some environments, leaving a session of Admin Console open but unattended for an extended length of time (such as overnight) might cause Admin Console to be unavailable to all users.

Solution:

Follow these steps to restart service_host:

1. Open Infrastructure Manager and log in to the domain as an administrator.

2. Expand the hub that hosts service_host (typically the primary hub) and display its probes.

3. Right-click on the service_host probe and select **Restart**.

4. Wait for two to three minutes to allow service_host to fully restart.

5. Sign in to Admin Console.

Deploying Robots to AIX and zLinux

Problem:

You cannot use Unified Service Manager (USM) to automatically deploy robots to AIX or zLinux systems that were placed in your inventory through automated discovery.

Solution:

To deploy robots to AIX or zLinux systems, use one of the following methods:

- Use the Automated Deployment Engine (ADE) probe with an XML file. See "Bulk Deployment with the ADE Probe" in the *UIM Server Installation Guide*.

- Use the native installers. See "Installing Robots and Secondary Hubs on Linux or Solaris" in the *UIM Server Installation Guide*.

- Import an XML file in USM. See "Deploy Robots to System Listed in a File" in the *UMP Unified Service Manager* help.

data_engine v7.92 Admin Console GUI

The following fields in the data_engine 7.92 Admin Console GUI are non-functional:

- **data_engine** node:
  - **Delete historic data older than** field
- **Quality of Service** node:
  - **Override Daily Average Age** selection
  - **Daily Average Age** field

These fields will be enabled in a future release.

Discovery Password Authentication

Discovery Agent uses password authentication to connect to a target device over SSH. Discovery Agent cannot communicate with a device where SSH is configured for other authentication methods, such as keyboard-interactive. Discovery Agent also does not support public key authentication or challenge-response authentication.

Admin Console Cannot Accept SSL Certificate in UMP

Problem:

When launching Admin Console as a portlet within UMP for the first time, you receive a 501 error that the self-signed SSL certificate is untrusted, but the interface does not provide a way to accept the certificate and continue. This is due to a limitation on how some browsers handle SSL-certificates within a secure iframe.

This problem occurs when Admin Console is configured to use a self-signed SSL certificate to communicate with the service_host process.

Solution:

1. Open Admin Console stand-alone in a web browser. Either:

   - Browse to https://*<UIM_server_name_or_IP>*:8080/adminconsole.

   - In the error dialog in UMP (certificate is not trusted; unable to establish communication to *<URL>*), copy the URL and paste it into another browser window or tab.

2. You will see the same security message, but are able to accept the certificate.

3. Open Admin Console within UMP (on the same browser at the same IP address).

NIS Manager Link in Infrastructure Manager Does Not Work

Problem:

Clicking on the **NIS Manager** link in Infrastructure Manager results in this error message:
```
Error executing command: C:\Program Files
(x86)\Nimsoft\bin\NiSmgr.exe
```

The NIS Manager application has been removed from the product.

Solution:

Use the Discovery Wizard available in the USM portlet to configure discovery components.

Using SSH Password Authentication with OpenSUSE 12.x

Problem:

By default OpenSUSE disables password authentication for SSH.

Solution:

To use password authentication for SSH:

1. Open the /etc/sshd_config file.

2. Change **PasswordAuthentication no** to **PasswordAuthentication yes**.

If you do not use password authentication, you must use RSA public key authentication. See Parameter Values for host-profiles.xml in the installation guide for details.

PPM Not Supported on AIX

The PPM probe does not run on AIX hubs. To configuring robots and probes on, or under AIX hubs, use the web-based raw configure or legacy Infrastructure Manager.

Windows 2008 Permission Issues

Write privileges are required for writing to the UIM program folder (default is C:\Program files (x86)\Nimsoft). If you log on as a user without administrator privileges after installation, you must manually set these write privileges.

Fault Correlation Affected by Alarm Forwarding and Replication

Problem:

Fault Correlation is impacted by the configuration of hub alarm forwarding and NAS alarm replication.

Solution:

For the Fault Correlation application to provide accurate results, you must ensure that alarms and interface_poller messages from hubs in the applicable areas of your network topology are being forwarded to the hub where the Fault Correlation Engine (FCE) probe is running. You must use hub queues that include subjects alarm and interface_poller to forward the messages FCE requires. Use either POST or GET queues based on whether you want to push or pull messages from one hub to the next.

Important: Do not enable NAS alarm replication or forwarding when using FCE. Doing so causes alarms to be processed twice and yields unpredictable results.

UNIX Robot Communication Fails Due to Invalid /etc/hosts

Problem:

On Unix systems, robot communication over the network fails due to an invalid **/etc/hosts** file.

Solution:

Ensure the **/etc/hosts** file on any system hosting a Nimsoft robot, hub, server, or UMP instance contains a valid entry for the local machine. This must be a fully qualified hostname and IP address. If only loopback is defined (for example, localhost 127.0.0.1), then the controller probe on that system will be unaware of its own IP address, resulting in network communication failure.

Unable to Find Device in USM by IP Address

As part of 7.0 discovery server and discovery agent enhancements, a device with multiple IP addresses is now shown as a single device in Unified Service Manager (USM), not as multiple distinct devices per IP address. If you can't locate a device in USM by an IP address, try searching for it by name.

Localization

Translated strings are garbled in the installation log file (iaoutput.txt).

Installation

Java JRE Version Requirements

The UIM Server installer requires a 64-bit Java Runtime Environment. On all platforms EXCEPT Windows Server 2012, we recommend that you install the most recent version of 64-bit JRE SE 7.

Windows Server 2012 requires a version from **1.7.0_06** to **1.7.0_51**. With earlier versions, the OS platform is not properly detected. Version 1.7.0_55 or later can cause a fatal application error in the installation process.

Note: On Solaris, the 64-bit JRE is located one directory deeper than on other platforms:

- AMD64 systems: /usr/java/jre/bin/amd64
- SPARC systems: /usr/java/jre/bin/sparcv9

Discovery Agent and Other Probes Issue Alarm on Update

Problem:

Discovery Agent and some other probes may send a single information alarm when upgrading to the latest version of UIM Server.

Solution:

This alarm is benign and can be safely ignored.

The other probes depend on a queue created by Discovery Server. The queue may not be entirely operational when these probes activate, which causes the information alarm to be sent. The queue will come up in a short period of time.

UIM Server Installation fails on CentOS and OpenSuse

Problem:

NM Server installation fails on CentOS and OpenSUSE version 12.

Solution:

The Data Engine requires libstdc++.so.5 (libstdc++-3.3.4-11.x86_64.rpm).

To install the compatible library, execute:
```
yum install compat-libstdc++-33
```

Secondary Hubs Requirements for Web-based Configuration

To use Admin Console on a secondary hub, the following components must be deployed to the secondary hub:

- PPM

- service_host

- monitoring_services

- ids_services

- automated_deployment_engine

- admin_console

Recommendation: Ensure these components are deployed to each hub within your domain.

Probes Fail to Start After UIM Server Installation

- **Installation on Windows**

  After installation on Windows, some probes may not start due to lack of available system resources.

  To fix this, edit registry key HKEY_LOCAL_MACHINE\System \CurrentControlSet \Control \Session Manager\SubSystems\Windows:

```
%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512,Windows=On
SubSystemType=Windows ServerDll=winsrv:UserServerDllInitialization,3
ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off MaxRequestThreads=16
```

  Change the value **512** to **1024**.

  For more information, see the [User32.dll or Kernel32.dll fails to initialize](#) Microsoft support article.

- **Installation on all platforms**

  Several components are distributed and configured during installation. On slower systems, some probes might not be started after installation. This can be detected in Admin Console or Infrastructure Manager, and is fixed by manually activating the probe.

- **Upgrade on all platforms**

  If you upgrade UIM Server and you have UMP installed, restart the **wasp** and **dashboard_engine** probes to avoid any issue logging into UMP after the upgrade.

UMP Installation on MySQL

If you have a MySQL database, you must deactivate the QoS_processor probe before installing or upgrading UMP. Reactivate the probe after UMP is installed.

Name Resolution Conflicts on Debian v6 with ADE

By default Debian v6 uses the address 127.0.1.1 as the name resolution address. When a robot is deployed to a Debian 6 system using ADE, after system restart the robot will attempt to bind to 127.0.1.1 as the address it is available at. Use the following workaround to avoid contention for 127.0.1.1 on your Debian 6 system:

- When installing the robot *manually* or with *ADE*, you must go to the target system after installation and add the following line to the robot.cfg file:

      robotip = ip_address

   where **ip_address** is the desired IP address that the robot should bind to on the target machine.

- When deploying to Debian 6.0.5 using *XML*, you must define the **<robotip>ip_address</robotip>** option, where **ip_address** is the IP address that the robot should bind to on the target machine.

LDAP User and Group Requirements for Login

An LDAP user cannot log into UIM Server unless an Active Directory group to which the user belongs is associated with a UIM access control list (ACL).

Silent Install with SQL Server and Dynamic Ports Requires DB-PORT

If you are installing with MS SQL Server named instances and you are using dynamic ports, you cannot use the default port number (1433), as this will prevent data_engine from connecting to the database.

Data_engine will be green in Infrastructure Manager (because it is running) but the lack of connection will cause its queue to grow in size continuously.

If the default port was used:

1. In Infrastructure Manager, open the data_engine probe configuration GUI by double-clicking the data_engine object.

2. On the **Database** tab, delete the comma and port number (**,1433**) appended to the database server name.

3. Specify the correct port, then restart the probe.

Failed Solaris Installation Reduces Available Swap Space

If UIM Server installation is interrupted or fails for any reason, the installer files (/tmp/install.*) are not deleted. Because Solaris swap includes the /tmp directory, CA recommends that you manually delete these files before running the installer again.

Access Denied for Root User on Linux with MySQL

Problem:

When attempting to install UIM Server with a MySQL database, you may see the following error (or its equivalent) after you enter the database server information:

```
ERROR 1045 (28000): Access denied for user 'root'@'<your Nimsoft hostname>' (using password: YES)
```

This occurs either because remote privileges have not been established, or because the password identified for remote systems is not consistent with what is set on the database server locally.

Solution:

Perform these steps:

1. Log in to the MySQL database locally (on the actual server hosting MySQL).

2. To set up access from:

   ■ Any host, execute:

```
mysql > use mysql;
mysql > UPDATE user SET password=PASSWORD("<your password>") where User = 'root';
mysql > GRANT ALL PRIVILEGES ON *.* TO root@'%' IDENTIFIED BY '<your password>' WITH GRANT OPTION;
mysql > GRANT TRIGGER ON *.* TO root@'%' IDENTIFIED BY '<your password>';
mysql > GRANT SUPER ON *.* TO root@'%' IDENTIFIED BY '<your password>';
mysql > FLUSH PRIVILEGES
```

   ■ A particular host, execute these commands, replacing *HostX* with the name of your host:

```
mysql > use mysql;
mysql > UPDATE user SET password=PASSWORD("<your password>") where User = 'root' AND Host = 'HostX';
mysql > GRANT ALL PRIVILEGES ON *.* TO root@'HostX' IDENTIFIED BY '<your password>' WITH GRANT OPTION;
mysql > GRANT TRIGGER ON *.* TO root@'HostX' IDENTIFIED BY '<your password>';
mysql > GRANT SUPER ON *.* TO root@'HostX' IDENTIFIED BY '<your password>';
mysql > FLUSH PRIVILEGES;
```

Invalid IP Error when Installing Windows Infrastructure

Problem:

When you run **NimBUS Infrastructure.exe** to install the Windows robot, hub and dstribution server, you may see the following error:

```
Command Line IP is not valid: 127.0.0.1
```

Solution:

This error is harmless and can safely be ignored. Click **OK** and continue.

Chapter 6: NMSRN--Fixed Defects

Hub and Robot

- Hub 7.xx tunnel connections now react to network conditions and automatically reset in order to ensure optimal data flow throughout your system. For this reason, alarms based simply on a low-level tunnel's state at a given instant no longer provide value. Those alarms have been replaced with more powerful queue status alarms that can more accurately track and provide alerts on the on-going quality of the higher-level connection.

Data_engine

- Data_engine no longer restarts when Unix robots have the system time set to year 2038 and beyond.

- In the Admin Console configuration GUI, minor changes were made to *Scheduler* field names to address wording and consistency issues.

Discovery

- Reintroduced population of CM_SNMP_SYSTEM and CM_SNMP_INTERFACE tables with discovery agent results in order to restore pre-7.0 Service Oriented Configuration (SOC) functionality and enable ACE to automatically configure the interface_traffic and cisco_monitor probes.

- Discovery Server and Relationship Service do not properly handle Discovery Agent and Topology Agent moving from its primary hub to its secondary hub. Now a single Discovery Agent instance is maintained in the database with its configuration data.

- Discovery Server failed to get discovery information for a robot managing probes that did not have the "group" field set. This information is now obtained.

- An alarm was issued if an *attach* queue was not created for the probe_discovery subject, even if a *post* queue was configured. Now an alarm is issued only if neither an *attach* queue nor a *post* queue is configured for probe_discovery.

- Discovery Server correlation has been adjusted to account for Cisco ASA routers. New exclusions were added to the MAC address correlation configuration to account for Cisco ASA internal data interfaces.

- Discovery Server failed to resubscribe to a hub due to malformed *nametoip* requests.

Service_host

- Service_host components now close unneeded connections resulting from failed logins.

- Corrected an anomaly in which source name fields were populated with probe names. Source names are now populated correctly.

- Addressed problems logging in to Admin Console after UIM Server installation.